13 citations found. Retrieving documents...
Z. Shi and R. Lee, "*Bit Permutation Instructions for Accelerating Software Cryptography*," in Proc. IEEE Intl. Conf Applicationspecific Systems, Architectures and Processors, pp. 138--148, 2000.

This paper is cited in the following contexts:

Algorithm Exploration for Efficient Public-Key.. - Potlapally, Ravi, .. (2002) (Correct)

...on extensive algorithmic exploration and tuning of the underlying cryptographic algorithms as the mechanism to achieve these objectives. **The proposed techniques are complementary to, and can be applied in conjunction with, improvements in security mechanisms, protocols, and hardware architectures [7, 10, 11, 12, 13, 14, 15, 16].** For most secure wireless transactions, the processing at the client is dominated by the public key algorithm [7, 17] Hence, we focus on the encryption decryption operation used in most popular public key algorithms [3, 18] namely modular exponentiation . We present an extensive suite of ....

Z. Shi and R. Lee, "***Bit Permutation** Instructions for Accelerating Software Cryptography*," in Proc. IEEE Intl. Conf Applicationspecific Systems, Architectures and Processors, pp. 138--148, 2000.

Optimizing Public-Key Encryption for Wireless Clients - Nachiketh Potlapally Srivaths (2002) (1 citation) (Correct)

... **extensions to their products, typically based on the addition of application specific co processors and or peripherals [25] 26] Computer architects have researched domain specific instructions for security processing, with an aim to maximize efficiency without compromising programmability [27], 28] Our work on exploration and tuning of the underlying cryptographic algorithms is complementary to most of the above efforts, since it can be applied to the algorithms underlying any given security protocol, and running on any given programmable hardware platform.** Hence, we believe such ....

Z. Shi and R. Lee, "***Bit Permutation** Instructions for Accelerating Software Cryptography*," in Proc. IEEE Intl. Conf Application-specific Systems, Architectures and Processors, pp. 138--148, 2000.

System Design Methodologies for a Wireless.. - Ravi.. (2002) (5 citations) (Correct)

... **security extensions to their products, typically based on the addition of application specific coprocessors and or peripherals [36, 37] Computer architects have researched domain specific instructions for security processing, with an aim to maximize efficiency without compromising programmability [38, 39].** Our target architecture and the system level design methodologies presented here are complementary to most of the above efforts, and can enable high efficiency in security processing while maintaining programmability. 6. **CONCLUSIONS** We presented the system level design methodology used to ....

Z. Shi and R. Lee, "***Bit Permutation** Instructions for Accelerating Software Cryptography*," in Proc. IEEE Intl. Conf. Application-specific Systems, Architectures and Processors, pp. 138--148, 2000.

Performance Impact of Data Compression on Virtual Private.. - McGregor, Lee (2000) (2 citations) (Correct)

...work, researchers have improved the performance of secure network transactions using a variety of techniques. **By adding new instructions to conventional instruction set architectures, the number of instructions in software implementations of cryptographic algorithms can be significantly reduced [22].** In addition, the computation associated with many cryptographic protocols is highly parallelizable. **When** performing encryption or message authentication, a multiprocessor system can achieve nearly linear speedup by assigning individual packets or connections to single processing elements [15] ....

Shi, Z., and R. Lee, "***Bit Permutation** Instructions for Accelerating Software Cryptography*", Proceedings of the IEEE International Conference on Applicationspecific Systems, Architectures and Processors, July 2000.